

# The Practical Guide to HIPAA Privacy and Security Compliance

By Kevin Beaver and Rebecca Herold

Published by Auerbach Publications in December 2003

## TABLE OF CONTENTS

### SECTION 1 HIPAA ESSENTIALS

---

#### **1 Introduction to HIPAA**

How HIPAA Came to Be

What HIPAA Covers

Organizations that Must Comply with HIPAA

    Covered Entities

    What Does Healthcare Mean?

    What Are Covered Transactions?

    What Does Electronic Form Mean?

    Are You a Covered Healthcare Provider?

    Are You a Covered Healthcare Clearinghouse?

    Are You a Covered Entity Private Benefit Plan?

    Are You a Covered Government-Funded Health Plan Program?

    Hybrid Entities

    Business Associates

Compliance Deadlines

HIPAA Penalties and Enforcement

Insight into the Electronic Transactions and Code Sets Rule

Summary

Chapter 1: Practical Checklist

#### **2 Preparing for the HIPAA Changes**

Background

Managing Change

Creating the Mindset

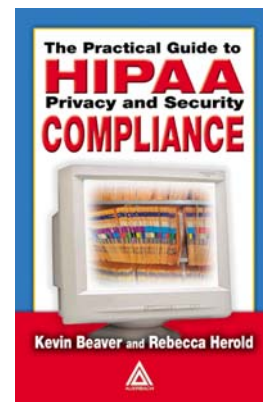
It's Up to You

Chapter 2: Practical Checklist

#### **3 HIPAA Cost Considerations**

Background

Privacy Implementation Costs



Privacy Ongoing Maintenance Costs  
Costs Related to Providing Access to PHI  
Privacy Officer Costs  
Security Implementation Costs  
Security Ongoing Maintenance Costs  
Security Officer Costs  
Chapter 3: Practical Checklist

#### **4 The Relationship between Security and Privacy**

Background

Privacy Rule and Security Rule Overlaps  
Appropriate and Reasonable Safeguards  
Protecting Appropriate Information  
Mapping PHI Data Flows  
Access Control and Information Integrity  
Assigned Security and Privacy Accountability  
Policies and Procedures  
Business Associate Agreements  
Training and Awareness  
Contingency Plans  
Compliance Monitoring and Audit  
Sanctions  
Individual Rights  
Access and Amendment  
Uses and Disclosures

Conclusion

Chapter 4: Practical Checklist  
Section 1: HIPAA Essentials Quiz

### **SECTION 2 HIPAA PRIVACY RULE**

---

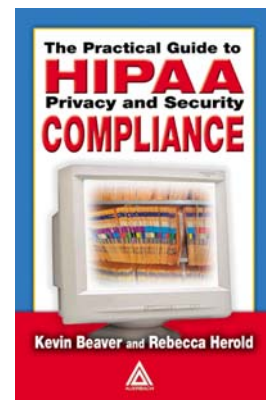
#### **5 HIPAA Privacy Rule Requirements Overview**

Background

Uses and Disclosures

General Rules for PHI Uses and Disclosures  
Uses and Disclosures: Organizational Requirements  
Uses and Disclosures: Consent for TPO  
Uses and Disclosures: Authorization  
Uses and Disclosures Requiring Opportunity for the Individual to Agree or Object  
Other Requirements Relating to Uses and Disclosures of PHI  
Limited Data Set  
Fundraising  
Underwriting Purposes  
Public Health  
Research  
Workers' Compensation

Incidental Uses and Disclosures



- Minimum Necessary
  - Reasonable Reliance
- De-Identification
- Business Associates
- Marketing
- Notice of Privacy Practices for PHI
- Individual Rights to Request Privacy Protection for PHI
- Individual Access to PHI
- Amendment of PHI
- Accounting Disclosures of PHI
- PHI Restrictions Requests
- Administrative Requirements
  - Privacy Officer
  - Training
  - Safeguards
  - Complaints
  - Sanctions
  - Mitigation
  - Refraining from Intimidating or Retaliatory Acts
  - Waiver of Rights
  - Policies and Procedures
  - Documentation
- Personal Representatives
- Minors
  - Some Points from HHS Regarding Personal Representatives and Minors
- Transition Provisions
- Compliance Dates and Penalties
- Looking Forward
- Chapter 5 Practical Checklist

## **6 Performing a Privacy Rule Gap Analysis and Risk Analysis**

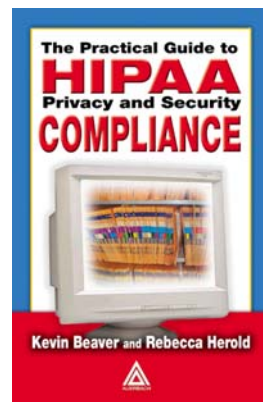
- Gap Analysis and Risk Analysis
- Chapter 6: Practical Checklist

## **7 Writing Effective Privacy Policies**

- Notice of Privacy Practices
- Example NPP
  - Header
  - Content of the Notice
- Layered Notices
- Before You Post or Distribute Your Notice
- Example Notice
- Organizational Privacy Policies
- Chapter 7: Practical Checklist

## **8 State Preemption**

- What Is Contrary?



Exceptions to Preemption  
Preemption Analysis  
    Framework for Analyzing HIPAA Preemption Issues  
Conclusion  
Chapter 8: Practical Checklist

## **9 Crafting a Privacy Implementation Plan**

Some Points to Keep in Mind  
Conclusion  
Chapter 9: Practical Checklist

## **10 Privacy Rule Compliance Checklist**

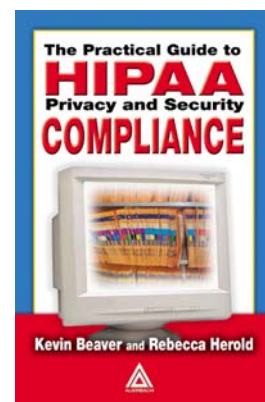
A. Prohibited Disclosures  
B. Disclosures Requiring Opportunity to Agree or Object  
C. Disclosures for treatment, payment, and operations (TPO)  
D. Disclosures Requiring Authorization  
E. Minimum Necessary Disclosure  
F. Notice  
G. Access  
H. Amendment  
I. Personal Representatives  
J. Confidential Communications Channels  
K. Accounting of Disclosures  
L. Complaint Process  
M. Prohibited Activities  
N. Safeguards  
O. Training  
P. Authentication  
Q. Mitigation  
R. Mandatory Documentation  
S. Demonstrating Compliance  
T. Business Associate Agreements  
U. Disclosures for Research, Marketing, and Fundraising  
V. Hybrid Entities  
W. Group Health Plans  
X. Healthcare Clearinghouses  
Y. Public Interest Disclosures  
Z. De-Identified Data Disclosures  
AA. Organized Healthcare Arrangements  
Section 2: HIPAA Privacy Rule Quiz

## **SECTION 3 HIPAA SECURITY RULE**

---

### **11 Security Rule Requirements Overview**

Introduction to the Security Rule  
What's New in the Final Security Rule  
    Key Terms Referenced in the Security Rule



General Rules for Security Rule Compliance  
Required vs. Addressable  
Insight into the Security Rule  
Other Organizational Requirements  
Reasons to Get Started on Security Rule Initiatives  
Chapter 11: Practical Checklist

## **12 Performing a Security Rule Risk Analysis**

Background  
Risk Analysis Requirements According to HIPAA  
Risk Analysis Essentials  
Stepping through the Process  
Calculating Risk  
Managing Risks Going Forward  
Chapter 12: Practical Checklist

## **13 Writing Effective Information Security Policies**

Introduction to Security Policies  
Critical Elements of Security Policies  
Sample Security Policy Framework  
Security Policies You May Need for HIPAA Security Rule Compliance  
Managing Your Security Policies  
Chapter 13: Practical Checklist

## **14 Crafting a Security Implementation Plan**

Background  
Some Points to Keep In Mind  
Conclusion  
Chapter 14: Practical Checklist

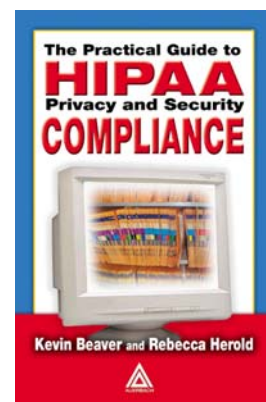
## **15 Security Rule Compliance Checklist**

Administrative Safeguard Requirements

- A. Security Management Process
- B. Assigned Security Responsibility
- C. Workforce Security
- D. Information Access Management
- E. Security Awareness and Training
- F. Security Incident Procedures
- G. Contingency Plan
- H. Evaluation
- I. Business Associate Contracts and Other Arrangement

Physical Safeguard Requirements

- J. Facility Access Controls
- K. Workstation Use
- L. Workstation Security
- M. Device and Media Controls



Technical Safeguard Requirements  
N. Access Control  
O. Audit Controls  
P. Integrity  
Q. Transmission Security  
Section 3: HIPAA Security Rule Quiz

## **SECTION 4 COVERED ENTITY ISSUES**

---

### **16 Healthcare Provider Issues**

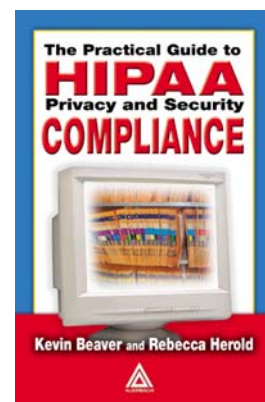
Background  
Privacy Notices  
Fees for Record Review  
Mitigation Measures  
Fax Use  
Sign-In Sheets  
Patient Charts  
Business Associates  
Authorizations  
    Marketing  
        Healthcare Provider Marketing Checklist  
        Fundraising  
Chapter 16: Practical Checklist

### **17 Healthcare Clearinghouse Issues**

Background  
Requirements  
Transactions  
Financial Institutions  
Conclusion  
Chapter 17: Practical Checklist

### **18 Health Plan Issues**

What Is a Health Plan?  
What Is a Small Health Plan?  
Health Plan Requirements  
Marketing Issues  
    A Health Plan Marketing Checklist  
Notice of Privacy Practices  
    A Health Plan Notice of Privacy Practices Checklist  
Types of Insurance Plans Excluded from HIPAA  
Communications  
Government and Law Enforcement  
    Government Departments  
    Government Enforcement  
    Debt Collection Agencies  
    Law Enforcement



Multi-State Issues  
Chapter 18: Practical Checklist

## **19 Employer Issues**

Background  
“Small” and “Large” Employers  
    Small Employer Issues  
Health Benefits  
Enforcement and Penalties  
Organizational Requirements  
    Employer Obligations as CEs  
    Employer Obligations as Plan Sponsors  
    Employer Organizational Requirements  
Health Information  
Medical Surveillance  
Workers’ Compensation  
    HIPAA and Workers’ Compensation Checklist  
Training  
Resources  
Conclusion  
Chapter 19: Practical Checklist

## **20 Business Associate Issues**

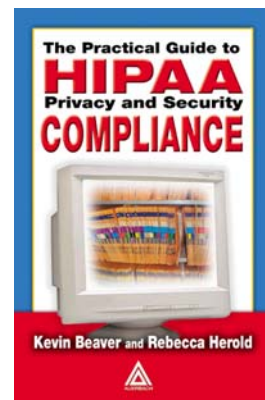
Is Your Organization a Business Associate?  
Business Associate Requirements  
What You Can Expect to See or Hear from Covered Entities  
Issues to Consider  
Moving Forward  
Chapter 20: Practical Checklist  
Section 4: Covered Entity Issues Quiz

## **SECTION 5 HIPAA TECHNOLOGY CONSIDERATIONS**

---

### **21 Building a HIPAA-Compliant Technology Infrastructure**

Overview  
Caution  
Areas of Technology to Focus On  
Looking Deeper into Specific Technologies  
    Access Controls  
    Antivirus and Malicious Code Protection  
    Applications and Databases  
    Data Backups and Storage  
    Encryption  
    Faxes  
    Firewalls



- Intrusion-Detection Systems
- Modems
- Operating Systems
- Personal Firewall/IDS Software
- Logging
- Passwords
- Messaging
  - E-Mail
  - Instant Messaging (IM)
- Remote Access/Virtual Private Networks
- Physical Security
- Mobile Computing Concerns
  - Wireless Networks
    - Technical Concerns
    - Security Concerns
    - What Can Be Done to Secure Wireless Networks?
  - Personal Digital Assistants
    - How Are the PDAs Used?
    - PDA Risks
    - Securing Health Information on PDAs
- Summary
- Chapter 21: Practical Checklist

## **22 Crafting Security Incident Procedures and Contingency Plans**

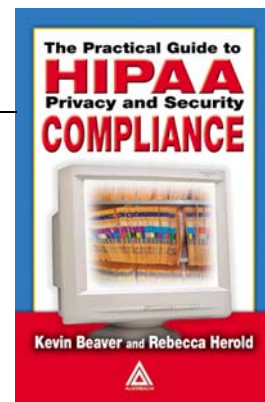
- Background
- Handling Security Incidents
- Security Incident Procedure Essentials
  - Response and Reporting (Required)
- Basics of Contingency Planning
  - Data Backup Plan (Required)
  - Emergency Mode Operation Plan (Required)
  - Testing and Revision Procedure (Addressable)
  - Applications and Data Criticality Analysis (Addressable)
- Moving Forward
- Chapter 22: Practical Checklist

## **23 Outsourcing Information Technology Services**

- Background
- Reasons to Consider Outsourcing
- What Functions to Outsource
- What to Look for in Outsourcing Firms
  - Questions to Ask Outsourcing Firms
- Common Outsourcing Mistakes
- Chapter 23: Practical Checklist
- Section V: HIPAA Technology Considerations Quiz

## **SECTION 6 MANAGING ONGOING HIPAA COMPLIANCE**

---





## **24 HIPAA Training, Education, and Awareness**

Creating an Effective Awareness Program

Identify Awareness and Training Groups

Training

    Specialized HIPAA Topics

    Training Delivery Methods

Training Design and Development

    Design and Development

Awareness Options

Document Training and Awareness Activities

Get Support

Measure Effectiveness

Conclusion

Chapter 24: Practical Checklist

## **25 Performing Ongoing HIPAA Compliance Reviews and Audits**

Background

Privacy Issues

Security Issues

Making Audits Work

Chapter 25: Practical Checklist

Section VI: Managing Ongoing HIPAA Compliance Quiz

## **SECTION 7 APPENDICES**

---

### **A. Case Studies**

Case 1: Healthcare Clearinghouse

Case 2: Metropolitan Area Healthcare System Case Study

Case 3: Small Physician's Office

Case 4: Multi-State Health Insurance Plan

### **B Sample Documents**

HIPAA Privacy Officer Job Description

    The Privacy Officer Role

Sample Chief Privacy Officer (CPO) Job Description

    Goal

    Qualifications

    Roles and Responsibilities

Sample HIPAA Security Officer Job Description

    Actions and Accountabilities

    General Skills and Experience Requirements

Sample HIPAA Business Associate Agreement

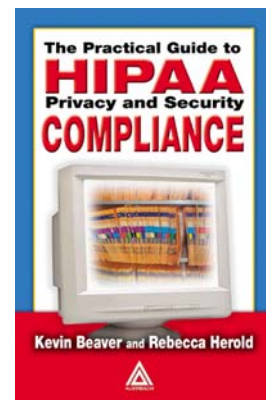
HIPAA Business Associate Agreement

    Recitals

HIPAA Privacy and Security-Specific Policies

    Sample Privacy Policies

    Uses and Disclosures of Protected Health Information



Notice of Privacy Practices  
Restriction Requests  
Minimum Necessary Disclosure of Protected Health Information  
Access to Protected Health Information  
Access to Protected Health Information by the Individual  
Amendment of Incomplete or Incorrect Protected Health Information  
Disclosure Accounting  
    Marketing Activities  
Prohibited Activities  
Business Associates  
    Training and Awareness  
    Sanctions  
Retention of Records  
Sample Security Policies  
Emergency Mode Operation  
Access Authorization to Systems Components  
Access Authorization  
Computer Systems Access Controls  
Internal Audits  
Background Checks  
Personnel Security: Visitor Escorts  
Security Configuration Management  
Computer Emergency Response  
Risk Assessments  
Contractor Termination Procedures  
Media Removal

## **C HIPAA Resources**

### **D Answers to Chapter Quizzes**

Section 1: HIPAA Essentials Quiz  
Section 2: HIPAA Privacy Rule Quiz  
Section 3: HIPAA Security Rule Quiz  
Section 4: Covered Entity Issues Quiz  
Section 5: HIPAA Technology Considerations Quiz  
Section 6: Managing Ongoing HIPAA Compliance Quiz

### **E HIPAA Glossary**

General and Miscellaneous Terms  
From the Regulatory Text

§ 162.103  
§ 160.103  
§ 160.202  
§ 142.103  
§ 164.501  
§ 164.504  
§ 142.304

